REGOLAMENTO PER LA GESTIONE RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE IN RSE

[regolamento V.00]

REGOLAMENTO PER LA GESTIONE RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE IN RSE	
Normativa e documenti interni richiamati	• Regolamento (UE) 2024/1689, c.d. AI ACT • Regolamento (UE) 2016/679, c.d. GDPR • D. Lgs. 30 giugno 2003, n. 196 recante il Codice in materia dei dati personali • Direttiva (UE) 2022/2555, c.d. "NIS 2" e D. Lgs. 4 settembre 2024 n. 138 • Legge n. 90/2024 rafforzamento della cybersicurezza nazionale e di reati informatici • D. Lgs. 10 febbraio 2005, n. 30 recante il Codice della proprietà industriale • D. Lgs. 8 giugno 2001, n. 231 recante la disciplina sulla responsabilità amministrativa degli enti • Contratto Collettivo Nazionale di Lavoro del settore elettrico (CCNL) • Orientamenti etici per un'IA affidabile emanati dal HLEG IA • *Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)* • *Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689* • *Living guidelines on the responsible use of generative AI in research* • Codice Etico di RSE
Storico delle versioni	Prima emissione
Approvato e aggiornato dall'Amministratore Delegato il 27.03.2025	

INDICE

1. PREMESSE

RSE, quale organismo di ricerca, ha un ruolo cruciale nel promuovere e stimolare l'utilizzo dell'Intelligenza Artificiale (IA), in particolare nell'ambito delle attività di ricerca scientifica e pertanto intende adottare e sperimentare i sistemi più utili a conseguire significativi miglioramenti in termini di efficienza operativa, qualità dei servizi, capacità d'innovazione.

La rapida e inarrestabile evoluzione delle attuali tecnologie e il loro dirompente potenziale, si impongono come centrali ed ineliminabili nelle dinamiche dell'innovazione e dello sviluppo, ma, nello stesso tempo, comportano implicazioni importanti e delicate che hanno reso necessario un intervento prolifico del legislatore nazionale ed europeo per poterne disciplinare le diverse ricadute.

Al fine di contemperare l'esigenza di RSE di evolvere al passo con lo sviluppo dei nuovi sistemi e quella di non incorrere in rischi di sicurezza o di violazioni di diritti e normative, è stato costituito un Gruppo di Lavoro "Progetto IA" (GdL PIA), con competenze trasversali, a cui è stato affidato il compito di provvedere ad analizzare il contesto esterno e interno sotto i differenti profili (tecnologici, legali, di cybersicurezza, economici, operativi, etici) al fine di individuare e monitorare nel tempo le esigenze aziendali, gli strumenti offerti dal mercato, l'evoluzione della normativa e delle migliori prassi in uso, con l'obiettivo di declinare, in modo efficiente, organizzato e sostenibile, l'uso delle nuove tecnologie di IA in RSE.

2. SCOPO DEL REGOLAMENTO

Il presente Regolamento, elaborato nell'ambito delle azioni del Gruppo di Lavoro, intende definire le linee guida per l'utilizzo dei sistemi di IA[1] in RSE, al fine di garantirne un uso etico, sicuro e trasparente sia con riferimento alle attività di gestione della società che, più in particolare, nell'ambito della ricerca scientifica, dando piena applicazione a quanto previsto dal Regolamento europeo sull'Intelligenza Artificiale.

Il Regolamento recepisce le indicazioni derivanti oggi dal quadro normativo nazionale e sovranazionale vigente che è, però, in piena fase evolutiva; si tratta, quindi, di uno strumento vivo, che sarà soggetto a periodica revisione e interpretazione evolutiva, al fine di adeguarne l'applicazione agli sviluppi normativi.

Il presente documento individua, nello specifico, i principi e le prescrizioni a cui attenersi, nonché i limiti e le preclusioni di utilizzo da rispettare per non incorrere in esposizione di rischio individuale o aziendale.

Gli scopi principali sono quelli di:

[1] Ai sensi dell'art. 3, comma 1, punto 1) AI Act, per sistema di IA si intende "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali"; si vedano altresì le linee guida elaborate dalla Commissione Europea sul punto "*Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689*".

- fornire indicazioni chiare per il corretto utilizzo dei sistemi di IA nelle proprie attività lavorative quotidiane, sia che si tratti di strumenti ufficialmente adottati dall'azienda, attraverso l'acquisizione di apposite licenze (es. Microsoft Copilot 365), sia che si tratti di strumenti utilizzati o sviluppati autonomamente dal singolo utente con i dispositivi messi a disposizione dall'azienda o comunque attraverso i sistemi informatici aziendali;
- individuare i criteri normativi e tecnici a cui attenersi per valutare la preliminare ammissibilità dell'utilizzo di sistemi di IA diversi da quelli già in uso.

3. QUADRO NORMATIVO

Il presente Regolamento tiene conto dell'attuale quadro normativo di riferimento che, per quanto già piuttosto articolato, è destinato a incrementare esponenzialmente la propria complessità nel corso dei prossimi anni, in vista dell'emanazione, già programmata, di decine di decreti e linee guida diretti, rispettivamente, all'attuazione e interpretazione della normativa recentemente entrata in vigore.

- **EU AI Act – Regolamento (UE) 2024/1689**: l'Unione Europea ha adottato il 13 giugno 2024 il Regolamento n. 2024/1689 sull'intelligenza artificiale, cosiddetto "AI Act" che stabilisce norme armonizzate per assicurare che i sistemi di IA utilizzati all'interno dell'Unione Europea siano completamente in linea con i diritti e i valori della stessa, garantendo il controllo umano, la sicurezza, il corretto trattamento dei dati personali, la trasparenza, la non discriminazione e il benessere sociale e ambientale.

  L'AI Act prevede un'applicazione differita delle diverse prescrizioni introdotte, alcune delle quali sono già entrate in vigore, mentre altre diverranno efficaci, con gradualità variabile, nell'arco di un biennio.

  Lo stesso AI Act prevede, inoltre, l'emanazione di circa 60 provvedimenti di secondo livello per dare attuazione e completare il mosaico disciplinare dallo stesso previsto.

  A completamento delle prescrizioni dell'AI Act, la Commissione Europea è già intervenuta con l'emanazione delle prime due **Linee Guida** relative, rispettivamente, a:

  1. le pratiche vietate nell'uso dei sistemi di IA ("***Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689***");
  2. la definizione di sistemi di IA ai fini dell'applicazione dei vincoli di cui all'AI Act ("***Guidelines on the definition of an artificial intelligence system established by Regulation (EU)***").

  Tali orientamenti, seppure non vincolanti, costituiscono la più autorevole fonte interpretativa a cui attenersi nell'applicazione delle disposizioni del Regolamento Europeo.
- **Direttiva NIS2 – Direttiva (UE) 2022/2555**: la Direttiva, recepita in Italia con Decreto legislativo 4 settembre 2024, n. 138, ha introdotto regole più stringenti per le aziende che operano all'interno dell'Unione

Europea con l'obiettivo di rafforzare la sicurezza informatica delle reti e dei sistemi informativi e di ottimizzare il processo di reporting degli incidenti.

- **Legge 28 giugno 2024, n. 90** recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici".
- **"*Living guidelines on the responsible use of generative AI in research*"**, adottate dalla Commissione Europea il 20 marzo 2024.
- ***General Data Protection Regulation* (GDPR) - Regolamento (UE) 2016/679:** il Regolamento Europeo in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

4. PRINCIPI GENERALI

Dal complesso normativo vigente sono desumibili i seguenti principi generali a cui il presente Regolamento fa costante riferimento nel disciplinare implementazione e uso dell'IA:

- **Etica e trasparenza**: l'uso responsabile dei sistemi di IA deve rispettare i principi etici e le normative vigenti e perseguire obiettivi valoriali condivisi nell'Unione Europea. Deve inoltre garantire la trasparenza nei processi decisionali garantendo un'adeguata tracciabilità e spiegabilità, consentendo agli utenti di essere informati quando interagiscono con un sistema di IA e ai terzi di conoscere un output generato tramite l'intelligenza artificiale.
- **Privacy e sicurezza**: devono essere adottate misure tecniche e organizzative adeguate a proteggere i dati personali (soprattutto se appartenenti a categorie particolari) e a garantire la sicurezza delle informazioni condivise ed elaborate.
- **Alfabetizzazione e consapevolezza**: l'utilizzo dei sistemi di IA deve essere orientato nell'ottica della gestione consapevole, tramite un processo di alfabetizzazione che porti l'utente a comprendere e riconoscerne il valore, il potenziale nelle decisioni aziendali e per gli impieghi lavorativi, i rischi ad essi collegati.
- **Intervento e sorveglianza umani**: l'utilizzo dei sistemi di IA deve essere implementato in modo da assicurare l'autonomia e il processo decisionale umano. Ciò potrà avvenire mediante meccanismi di governance che consentano l'intervento umano nel ciclo decisionale oppure mediante un controllo e la supervisione umana.
- **Robustezza tecnica e sicurezza**: l'implementazione e utilizzo in azienda di sistemi di IA deve garantire che gli stessi siano sicuri e affidabili dal punto di vista tecnico e sociale e la minimizzazione del rischio di danno involontario.

- **Riservatezza e governance dei dati:** RSE provvede a mappare e classificare le informazioni aziendali in base al livello di riservatezza al fine di assicurare la protezione dei dati confidenziali e personali. RSE elabora i dati aziendali in modo da soddisfare livelli elevati in termini di qualità e integrità.
- **Inclusione, non discriminazione ed equità**: gli strumenti adottati in azienda devono essere sviluppati e utilizzati in modo da promuovere l'inclusione, la parità di accesso, l'equità di genere, evitando ogni possibile effetto discriminatorio e pregiudizievole.
- **Accountability:** RSE è responsabile della corretta implementazione e del monitoraggio di conformità sui sistemi di IA che sono stati autorizzati e delle eventuali conseguenze pregiudizievoli che ne possono derivare. I singoli utenti dei sistemi di IA sono responsabili dell'uso corretto e appropriato delle tecnologie di IA, in conformità alla normativa, al Codice Etico, alle policy aziendali e in particolare al presente Regolamento.

5. AMBITO DI APPLICAZIONE

Il presente Regolamento si applica a tutti i dipendenti o equiparati, collaboratori, professionisti, clienti, partner e fornitori della società che utilizzano o intendono utilizzare sistemi di IA nell'ambito della attività svolte per conto di RSE o in collaborazione con essa.

Si applica altresì a tutti i sistemi di IA ricompresi nella definizione di cui all'art. 3 comma 1, punto 1) dell'AI ACT, siano essi sistemi ad alto rischio, modelli di IA per finalità generali, sistemi di IA generativa, o altri sistemi comunque definiti all'interno del sopra richiamato Regolamento europeo.

Sono inclusi i sistemi sviluppati da partner e/o fornitori di RSE e quelli sviluppati ed implementati internamente al solo fine di supportare e migliorare qualitativamente l'attività di ricerca scientifica svolta. In questa seconda eventualità, trattandosi di sistemi di IA sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici, esulano dall'ambito di applicazione dell'AI ACT, come stabilito dal Considerando n. 25del Regolamento[2].

[2] Il Considerando n. 25 recita: "Il presente regolamento dovrebbe sostenere l'innovazione, rispettare la libertà della scienza e non dovrebbe pregiudicare le attività di ricerca e sviluppo. È pertanto necessario escludere dal suo ambito di applicazione i sistemi e i modelli di IA specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici. È inoltre necessario garantire che il regolamento non incida altrimenti sulle attività scientifiche di ricerca e sviluppo relative ai sistemi o modelli di IA prima dell'immissione sul mercato o della messa in servizio. Per quanto riguarda le attività di ricerca, prova e sviluppo orientate ai prodotti relative ai sistemi o modelli di IA, le disposizioni del presente regolamento non dovrebbero nemmeno applicarsi prima che tali sistemi e modelli siano messi in servizio o immessi sul mercato. Tale esclusione non pregiudica l'obbligo di conformarsi al presente regolamento qualora un sistema di IA che rientra nell'ambito di applicazione del presente regolamento sia immesso sul mercato o messo in servizio in conseguenza di tale attività di ricerca e sviluppo, così come non pregiudica l'applicazione delle disposizioni sugli spazi di sperimentazione normativa per l'IA e sulle prove in condizioni reali. Inoltre, fatta salva l'esclusione dei sistemi di IA specificamente sviluppati e messi in servizio solo a scopo di ricerca e sviluppo in ambito scientifico, qualsiasi altro sistema di IA che possa essere utilizzato per lo svolgimento di qualsiasi attività di ricerca e sviluppo dovrebbe rimanere soggetto alle disposizioni del presente regolamento. In ogni caso, qualsiasi attività di ricerca e sviluppo dovrebbe essere svolta conformemente alle norme etiche

6. IMPLEMENTAZIONE E UTILIZZO DI SISTEMI DI IA IN AZIENDA

6.1 Autorizzazione e controllo sul corretto utilizzo

L'implementazione e/o l'utilizzo in azienda di nuovi sistemi o strumenti di IA devono essere preventivamente autorizzati.

I sistemi o strumenti precedentemente adottati saranno soggetti alla procedura di verifica a posteriori per l'eventuale autorizzazione in ratifica.

L'iter autorizzativo prevede:

- mappatura e valutazione dei potenziali rischi associati a ciascun utilizzo;
- adozione di specifiche istruzioni/misure per la mitigazione dei rischi identificati;
- controllo sul corretto utilizzo ed eventuali anomalie;
- tracciamento e monitoraggio dei sistemi in uso in azienda;
- interventi formativi adeguati agli strumenti in uso.

Il processo autorizzativo, seguendo le indicazioni fornite dal GdL "Progetto IA", deve tenere conto di tutte le implicazioni di carattere tecnologico, di sicurezza, normative e operative e coinvolgere opportunamente, in ogni passaggio, tutte le Unità competenti.

Qualora un utente intenda proporre l'adozione di un nuovo sistema di IA deve inserire apposita istanza nei gestionali aziendali e, attenendosi alle procedure aziendali, fornire tutte le informazioni richieste nel corso dell'intero iter di verifica e autorizzazione.

Ciascuna Unità coinvolta in fase di verifica può subordinare il rilascio della propria autorizzazione al rispetto di specifiche prescrizioni che si rendano di volta in volta necessarie ad assicurare la compliance o la funzionalità aziendale dello strumento in valutazione.

L'approvazione finale spetta al coordinatore del GdL, "Progetto IA", previa condivisione all'interno del Gruppo.

6.2 Mappatura e valutazione dei rischi

La mappatura dei rischi deve tenere conto di tutte le possibili implicazioni derivanti dall'utilizzo di un sistema di IA nell'ambito delle attività di RSE.

e professionali riconosciute nell'ambito della ricerca scientifica e dovrebbe essere condotta conformemente al diritto dell'Unione applicabile".

6.2.1 Qualificazione dei rischi secondo l'AI Act

Le Unità coinvolte nel flusso autorizzativo dovranno attenersi, in primo luogo, alle indicazioni stabilite dall'AI Act e adottare un analogo approccio *risk-based* in base alla qualificazione dei quattro livelli di rischio individuati dalla normativa europea.

Rischio inaccettabile	**Sono strettamente vietate** le applicazioni che, secondo la categorizzazione operata dal richiamato Regolamento Europeo, espongono ad un rischio qualificabile come "inaccettabile", come meglio precisato dalle richiamate Linee Guida adottate dalla Commissione Europea. Rientrano in tale classificazione le soluzioni che perseguono l'obiettivo di orientare o distorcere i comportamenti utilizzando tecniche subliminali, manipolative o ingannevoli o sfruttando le vulnerabilità soggettive o sociali; i sistemi volti a classificare o assegnare punteggi alle persone in base ai comportamenti sociali o alle caratteristiche personali; i sistemi predittivi di criminalità basati sulla profilazione o su tratti e caratteristiche della personalità; i sistemi che creano o ampliano banche dati di riconoscimento facciale attraverso lo *scraping* di immagini facciali da Internet o da filmati di telecamere a circuito chiuso; le soluzioni di riconoscimento emotivo e quelle dirette alla categorizzazione delle persone in base a dati biometrici; i sistemi di riconoscimento facciale biometrico da remoto, in tempo reale e in spazi accessibili al pubblico.
Rischio elevato	**Sono preclusi in RSE** l'implementazione e l'utilizzo di soluzioni di IA che espongono ad un rischio definito dall'AI Act come "elevato", come elencati nell'Annex III dell'AI Act. Rientrano in tale classificazione le soluzioni di identificazione biometrica (non vietate); i sistemi utilizzati nell'ambito delle infrastrutture digitali critiche, del traffico stradale o nella fornitura di acqua, gas, riscaldamento o elettricità; le soluzioni utilizzate nell'ambito dell'istruzione e formazione professionale o dell'occupazione, gestione e reclutamento dei lavoratori; i sistemi utilizzati nell'ambito dei servizi privati essenziali, prestazioni e servizi pubblici essenziali; sistemi utilizzati dalle forse di pubblica sicurezza o da altre istituzioni che intervengono a loro sostegno; quelli utilizzati dalle autorità e istituzioni nell'ambito delle politiche di migrazione, asilo e gestione del controllo delle frontiere; i sistemi adottati nell'ambito dell'amministrazione della giustizia e dei processi democratici. L'utilizzo di tali sistemi è consentito dalla legge a condizione che vengano rispettati importanti requisiti di carattere tecnologico e definiti chiari criteri di responsabilità in ordine alla valutazione iniziale e continua di conformità, alla valutazione di impatto sui diritti fondamentali degli individui (*Fundamental Rights Impact Assessment* – FRIA, art. 27 AI Act) al monitoraggio, alla supervisione umana, agli obblighi di trasparenza e alla registrazione di banca dati. All'attuale stadio dell'evoluzione normativa, molte delle prescrizioni necessarie a definire compiutamente le regole di conformità di sviluppo e utilizzo di tali soluzioni sono ancora in via di definizione. Per tali ragioni di incertezza normativa, l'adozione di questi sistemi è, al momento, preclusa in RSE e ne sarà riconsiderato il possibile utilizzo quando il quadro normativo sarà più stabile.
Rischio limitato	**Possono essere implementati e utilizzati in RSE, previa autorizzazione**, i sistemi di intelligenza artificiale che ricadono nella categoria di "rischio limitato". Sono tali le tecnologie e pratiche di IA, non ricomprese nelle precedenti categorie, capaci comunque di influenzare i diritti o le volontà degli utenti, ma in misura minore rispetto ai sistemi ad alto rischio. Ritroviamo in questa categoria i sistemi di IA

	utilizzati per generare o manipolare contenuti audiovisivi (come i *deepfake*), o di interagire con le persone fisiche per fornire suggerimenti personalizzati (come le *chatbot*). Tali soluzioni sono soggette a obblighi di trasparenza e consenso informato. Sono riconducibili a questo livello di rischio i sistemi di IA generativa, purché essi siano adottati nell'ambito di pratiche diverse da quelle individuate nelle precedenti categorie e siano rispettate le strategie di mitigazione dei rischi indicate nel presente Regolamento.
Rischio minimo	**Possono essere implementati e utilizzati in RSE, previa autorizzazione,** i sistemi di IA che rientrano nella categoria "di rischio minimo". Si tratta di soluzioni che non hanno alcun impatto diretto sui diritti fondamentali o sulla sicurezza delle persone e dei sistemi e offrono ampi margini di scelta e controllo agli utenti. Sono liberi da obblighi normativi specifici secondo l'AI Act e possono essere utilizzati con una supervisione regolamentare minima. Rientrano in questa categoria i filtri antispam e i sistemi utilizzati per scopi ludici o estetici.
Esclusioni	L'AI Act colloca poi al di fuori del proprio di ambito di applicazione i sistemi e i modelli di IA specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici (Considerando n. 25 AI Act). **Ne consegue che un sistema di IA sviluppato da RSE ed utilizzato esclusivamente all'interno dell'organizzazione aziendale a soli fini di ricerca scientifica, non immesso nel mercato né ceduto a terzi, non sarà soggetto ai divieti e alle prescrizioni imposte dalla richiamata norma europea, pur rimanendo soggetto alla procedura autorizzativa interna.** Residuano infatti, in ogni caso, implicazioni giuridiche e tecniche rilevanti e rischi in termini di trattamento di dati personali, sicurezza informatica, tutela della proprietà intellettuale e della riservatezza, controllo del lavoratore a distanza che richiederanno la verifica di conformità all'ulteriore normativa e ai regolamenti aziendali vigenti.

6.2.2 Trattamento dei dati personali, sicurezza informatica e informazioni riservate

L'adozione di un sistema di IA in azienda può comportare rischi per il trattamento di dati personali o di informazioni riservate. L'implementazione di *tool* che si integrino o accedano ai sistemi aziendali può, inoltre, comportare gravi rischi per la sicurezza dei sistemi informativi.

L'identificazione dei rischi associati allo specifico strumento potrebbe rendere necessario lo svolgimento di una valutazione di impatto sulla protezione dei dati personali (*Data Protection Impact Assessment* - DPIA) ai sensi dell'art. 35 GDPR.

L'iter di verifica e autorizzazione dovrà analizzare le fonti di rischio e indicare le specifiche misure organizzative e tecniche da implementare per contenere e mitigare tali rischi. Saranno inoltre indicate le prescrizioni a cui attenersi e la documentazione da produrre per garantire la piena compliance nell'uso del sistema di IA (es. informativa privacy ai sensi dell'art. 13 GDPR, relazioni informative per OO.SS., ecc.).

6.2.3 Proprietà intellettuale

Nell'adozione di un sistema di IA, in particolare se IA generativa, saranno considerati altresì i rischi derivanti da potenziali violazioni di diritti di proprietà intellettuale appartenenti a terzi e la necessità di tutelare il patrimonio immateriale di RSE da possibili condizioni contrattuali avverse o non trasparenti e da usi impropri.

Non potranno essere autorizzati i sistemi di IA generativa che non garantiscano livelli minimi di certezza in ordine alla proprietà degli output, alla riservatezza dei dati di input e alla tutela delle informazioni proprietarie. Laddove necessario, inoltre, potranno essere individuate specifiche prescrizioni per il corretto utilizzo dei sistemi autorizzati, anche ulteriori rispetto a quelle generali indicate nel presente Regolamento.

6.2.4 Trasparenza

Potranno essere autorizzati solo strumenti di IA sviluppati in modo da consentire un'adeguata tracciabilità[3] e spiegabilità[4] degli stessi. L'uso degli strumenti deve inoltre rendere consapevoli gli utenti di comunicare o interagire con un sistema di IA e dei limiti di tale sistema. Devono esser fornite informazioni chiare, accessibili e comprensibili sui diritti degli utenti e sulle modalità di trattamento dei dati.

6.2.5 Tutela dei lavoratori

L'adozione di IA all'interno dei contesti aziendali solleva questioni particolarmente delicate qualora venga utilizzata per la gestione del personale, del processo di assunzione e cessazione del rapporto lavorativo o nell'ambito della valutazione delle performance o dello sviluppo di carriera.

Come chiarito nel paragrafo 6.2.1, l'AI Act qualifica tali pratiche di utilizzo dell'IA come sistemi a "**rischio elevato"** per i quali RSE ha scelto, in via cautelativa, di rinviarne l'adozione al momento in cui si sarà stabilizzato il quadro normativo attualmente in evoluzione.

6.3 Alfabetizzazione, formazione e gestione consapevole

RSE si assicura che tutti gli utenti coinvolti nell'utilizzo dei sistemi di IA adottati in azienda ricevano una periodica e adeguata formazione sull'uso responsabile degli stessi, sui rischi ad essi collegati, con particolare riferimento a quelli correlati alla diffusione non autorizzata di dati personali o comunque riservati, sui protocolli di sicurezza, e sulla tutela della proprietà intellettuale, al fine di sensibilizzare tutto il personale sulle conseguenze derivanti da eventuali violazioni della normativa vigente o delle disposizioni del presente Regolamento.

---

[3] Il Considerando n. 27 dell'AI Act recita: "Con «trasparenza» si intende che i sistemi di IA sono sviluppati e utilizzati in modo da consentire un'adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA e informando debitamente i deployer delle capacità e dei limiti di tale sistema di IA e le persone interessate dei loro diritti".

[4] Per il concetto di spiegabilità si rinvia ai quattro principi elaborati dal *National Institute of Standards and Technology* (NIST) statunitense nel paper NISTIR 8312 "*Four Principles of Explainable Artificial Intelligence*", https://doi.org/10.6028/NIST.IR.8312.

Ciascun utente coinvolto dovrà partecipare alle iniziative formative programmate dall'azienda e sviluppare la capacità di leggere, utilizzare, analizzare, comunicare e proteggere i dati aziendali e/o di terzi inseriti nei sistemi di IA, in conformità con quanto richiesto dall'art. 4 dell'AI Act.

Tale capacità di "alfabetizzazione" agevola l'utilizzo critico dell'IA per mezzo dell'inserimento di prompt[5] adeguati e dell'identificazione e della verifica attenta degli output, al fine di scongiurare eventuali possibili allucinazioni[6] prodotte dal sistema.

7. DISCIPLINARE DI UTILIZZO DEI SISTEMI DI IA

Ogni utente è personalmente responsabile della quantità e qualità delle informazioni inserite nei prompt e per svolgere operazioni che prevedano l'utilizzo di sistemi di IA.

Nell'utilizzo dei sistemi di IA gli utenti dovranno attenersi scrupolosamente alle indicazioni dettate dall'azienda con questo Regolamento, con le procedure gestionali e note operative, nonché attraverso le specifiche prescrizioni eventualmente ricevute ad esito dell'iter approvativo.

7.1. Richiesta di autorizzazione

Ogni utente che intenda avvalersi di sistemi di IA disponibili sul mercato o sviluppati autonomamente, utilizzandoli sui dispositivi aziendali o, comunque, nell'ambito delle proprie attività di lavoro, dovrà preventivamente presentare apposita istanza attraverso i gestionali aziendali, attenendosi alle procedure delineate e avendo cura di fornire tutte le informazioni richieste nel corso dell'intero iter di verifica e autorizzazione.

Il sistema potrà essere utilizzato solo ad esito dell'iter autorizzativo.

7.2. Classificazione di confidenzialità delle informazioni di input

Gli utenti sono consapevoli che gli input caricati (testi, dati, messaggi, immagini, ecc.) potrebbero essere utilizzati per altri scopi, come l'addestramento di modelli di IA, pertanto, proteggono le informazioni aziendali non condivisibili e quelle di terzi facendo attenzione a non immetterle in un sistema di IA a meno che non vi sia la garanzia, come opportunamente verificato nell'iter approvativo dello strumento, che i dati non saranno riutilizzati (ad esempio per addestrare futuri modelli linguistici o per il riutilizzo non rintracciabile), che vi siano misure tecniche adeguate per la sicurezza e la protezione dei dati e che sia specificato dove e con quale livello di accessibilità e sicurezza siano ospitate le informazioni caricate.

RSE ha proceduto a mappare i dati in base al loro livello di riservatezza, definendo specifiche etichette ("Etichette di riservatezza"). La gestione di tali etichette avviene tramite la piattaforma Microsoft PureView, che

[5] Per "prompt" si intende un testo in linguaggio naturale che richiede all'IA generativa di eseguire un'attività specifica.

[6] Le allucinazioni si verificano quando un sistema di IA percepisce modelli o oggetti inesistenti o impercettibili agli osservatori umani, creando output privi di senso o del tutto imprecisi.

permette agli owner di processo di gestire i rischi relativi ai dati critici. L'integrazione di PureView e delle etichette di riservatezza con gli strumenti di lavoro e con i sistemi di IA in uso consente in automatico agli utenti finali di applicare la classificazione operata secondo le politiche di protezione dei dati adottate dall'azienda.
Gli utenti dei sistemi di IA sono tenuti a seguire tale classificazione avendo cura di elaborare i prompt in modo da non immettere dati o informazioni di input non condivisibili perché classificati come riservati, strettamente riservati o personali.

7.3. Tutela della proprietà intellettuale

Al fine specifico di tutelare i diritti di proprietà intellettuale di contributi attribuiti a soggetti terzi e scongiurare il rischio di plagio, l'utente deve verificare di avere le eventuali necessarie autorizzazioni degli autori alla rielaborazione dei contenuti tramite un sistema di IA o, comunque, all'utilizzo delle informazioni proprietarie (es. know-how), fornendo la corretta attribuzione e citazione delle fonti e rispettando le normative sul copyright e le licenze d'uso.
Sono vietate operazioni che non siano conformi con la disciplina in materia di brevetti, marchi o diritti d'autore.

7.4. Verifica dell'accuratezza di input e output

Ogni utente deve massimizzare la qualità delle informazioni inserite nei prompt al fine di ottenere un output quanto più possibile accurato.
Gli utenti sono consapevoli che l'output generato dai sistemi di IA a seguito dell'input/prompt ricevuto è comunque soggetto a errori o *bias* che possono determinare discriminazioni o allucinazioni nei risultati.
Gli utenti e, in particolare i ricercatori, mantengono un approccio critico all'utilizzo dei risultati prodotti dall'IA generativa e sono consapevoli dei limiti di tali strumenti. I sistemi di IA non sono né autori né coautori del risultato prodotto: la paternità dell'output implica la piena responsabilità degli utilizzatori dei sistemi di IA sui contenuti prodotti dai sistemi stessi.
Nell'ambito della ricerca scientifica, gli utenti sono tenuti a garantire che il materiale generato dall'IA non venga utilizzato in modo improprio, come ad esempio falsificando, alterando o manipolando i dati originali. Gli utenti hanno la responsabilità di assicurarsi che qualsiasi contenuto prodotto sia sottoposto a un attento controllo, verificando la qualità, l'originalità, la correttezza, l'accuratezza e l'assenza di discriminazioni.

7.5. Trasparenza

Per garantire la trasparenza dell'operato di RSE negli elaborati prodotti con un **contributo sostanziale dell'IA generativa,** gli autori devono rendere noti gli strumenti utilizzati indicandone i riferimenti principali (ad es. nome, versione, data) e il modo in cui essi sono stati utilizzati e hanno influenzato il processo di ricerca. Tenendo conto della natura stocastica (casuale) degli strumenti di IA generativa -ovvero della tendenza a produrre risultati

diversi a partire dallo stesso input- i ricercatori mirano alla riproducibilità e alla solidità dei risultati e delle conclusioni. Per tale ragione i ricercatori rendono noti o discutono i limiti degli strumenti di IA generativa utilizzati, comprese le possibili distorsioni nei contenuti generati, nonché le possibili misure di mitigazione.

7.6. Formazione e aggiornamento

Gli utenti dovranno rendersi disponibili alla formazione somministrata in azienda o richiedere formazione specifica laddove necessario per utilizzare correttamente gli strumenti di IA, in modo da massimizzarne i vantaggi e minimizzare i rischi.

La rapida evoluzione dei sistemi rende, inoltre, necessario un aggiornamento costante sulle migliori pratiche di utilizzo e le criticità emergenti.

7.7. Revisioni, valutazioni e referaggio

Nell'ambito della ricerca scientifica, deve essere evitato un ricorso sostanziale agli strumenti di IA generativa nell'ambito di attività che potrebbero avere un impatto sul lavoro di altri ricercatori o organizzazioni (ad esempio, *peer review*, valutazione di proposte di ricerca, ecc.). Ciò al fine di scongiurare rischi di trattamento o valutazione iniqua che possono derivare dai limiti di questi strumenti (quali allucinazioni e pregiudizi) e salvaguardare l'autenticità di contributi originali non ancora pubblicati.

8. REGISTRO DEI SISTEMI DI IA

Tutti i sistemi di IA, rinvenibili nel mercato, sviluppati internamente a RSE oppure sviluppati per conto di RSE, per i quali viene presentata istanza di implementazione o utilizzo in azienda – che siano stati o meno autorizzati – sono iscritti in un apposito registro a cura del Gruppo di Lavoro "Progetto IA".

Il Registro riporterà la descrizione del sistema adottato, la tecnologia e le funzionalità rilevanti, gli utenti coinvolti nel suo utilizzo, le finalità principali perseguite, la data di approvazione, la data dell'eventuale rigetto e delle sue motivazioni, le date di monitoraggio, la data e il motivo della dismissione.

9. MONITORAGGIO, REVISIONE E DISMISSIONE DEI PROGETTI IA

Il Gruppo di Lavoro, anche su impulso dei singoli utenti che utilizzano sistemi di IA, si occupa del monitoraggio periodico, dell'eventuale revisione e dismissione dei progetti che utilizzano IA.

10. CONFORMITÀ E SANZIONI

Le operazioni degli utenti svolte in maniera non conforme alla normativa vigente e al presente regolamento costituiscono violazioni sanzionabili ai sensi del Codice Disciplinare di RSE.

11. DISPOSIZIONI FINALI ED ENTRATA IN VIGORE

11.1 Disposizioni finali

Per quanto non espressamente previsto nel presente regolamento, trovano applicazione:

- le leggi ed i regolamenti nazionali ed europei;
- i contratti collettivi nazionali di lavoro del comparto;
- i regolamenti e le procedure aziendali.

Le norme del presente regolamento e la terminologia utilizzata si intendono modificate per effetto di norme sopravvenute.

Il presente regolamento, a seguito di apposito monitoraggio della sua applicazione, sarà soggetto a revisione periodica.

11.2 Entrata in vigore

Il presente Regolamento entra in vigore il giorno successivo alla sua approvazione da parte dell'Amministratore Delegato con acquisizione del relativo protocollo e non trova applicazione per le procedure avviate prima di tale data. Dall'entrata in vigore del Regolamento è abrogata ogni altra previgente disposizione aziendale che possa risultare in conflitto con le previsioni contenute nello stesso.